CLAIMS

What is claimed is:

1. A message encryption system comprising:

a session key employed to securely exchange a message associated with a dialog; and,

an encryption component that employs asymmetric encryption to first securely transmit the session key, the session key thereafter being employed to encrypt the message and securely exchange the message.

2. The system of claim 1, the session key comprising a 128-bit randomly generated symmetric key.

3. The system of claim 1, the encryption component first encrypts the session key employing a private key, the encryption component further encrypts the result of the first encryption employing a public key.

4. The system of claim 3, the private key being securely associated with an initiator of the message.

5. The system of claim 3, the public key being associated with a target of the message.

6. The system of claim 3, further comprising a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key.

7. The system of claim 6, a trusted agent negotiates a unique session key with a subscriber

8. The system of claim 6, the trusted agents acting in concert to dynamically load balance distribution for the publisher.

9. The system of claim 3, the public key being stored as a digital certificate.

10. The system of claim 9, the digital certificate being associated with a user *via* a login protocol.

11. The system of claim 1, the encryption component first encrypts the session key employing a private key, the encryption component further encrypts the result of the first encryption employing a public key, and, the encryption component separately encrypts the session key with a public key, the result of the second encryption and the separate encryption provided as an output.

12. The system of claim 1, the encryption component further encrypting the message with a private key.

13. A broker security system employing the session key of claim 1.

14. A message decryption system comprising:

a session key employed to securely exchange a message associated with a dialog; and,

a decryption component that employs asymmetric decryption to first securely decrypt the session key, the session key thereafter being employed to decrypt the message.

15. The system of claim 14, the decryption component first decrypts a message with a private key, the decryption component further decrypting the result of the first decryption with a public key, the result of the second decryption is the session key.

16. The system of claim 15, the private key being securely associated with a target of the message.

17. The system of claim 16, the public key being associated with an initiator of the message.

18. A method facilitating session key encryption comprising:
firstly encrypting a symmetric session key with a private key;
secondly encrypting a result of the first encryption with a public key; and,
providing a result of the second encryption as an output.

19. The method of claim 18, the private key being associated with an initiator of a message.

20. The method of claim 18, the public key being associated with a target of a message.

21. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 18.

22. A method facilitating session key decryption comprising:
firstly decrypting a message with a private key;
second decrypting a result of the first decryption with a public key; and,
employing a result of the second decryption as a session key.

23. The method of claim 22, the private key being associated with a target of a message.

24. The method of claim 22, the public key being associated with an initiator of a message.

25. A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 22.

26. A data packet transmitted between two or more computer components that facilitates secure distributed communication, the data packet comprising:

a data field comprising an encrypted message, the encrypted message first encrypted with a symmetric session

27. A message decryption system comprising:

means for receiving an encrypted session key;

means for decrypting the encrypted session key using a private key;

means for decrypting a result of the first decryption with a public key;

means for securely storing a result of the second decryption as a session key; and,

means for employing the session key to decrypt a message.